

クラウド時代における光通信の安全性を強化した暗号通信トランシーバ開発に成功！**玉川大学 量子情報科学研究所****世界初！****ランダム化機構組込のイーサネット対応の量子エニグマ暗号トランシーバを開発し ShowNet で相互接続****— 6月8日から開催される「Interop Tokyo 2016」で検証試験 —**

クラウド・システムの通信基盤となる光通信回線を保護する物理暗号の開発が求められている。

玉川大学（東京都町田市玉川学園 6-1-1 学長：小原芳明） 量子情報科学研究所の二見史生教授と加藤研太郎教授は、世界で初めて、ランダム化機構を組み込んだギガビットイーサネット (GbE) 対応の量子エニグマ暗号トランシーバ (TU Cipher-0) を開発した。

「Interop Tokyo 2016」に出展し、最先端の技術や製品などを結集する相互接続検証ネットワーク「ShowNet」に本トランシーバを接続し、検証試験を行う。また、本技術の詳細は国際会議「SPIE Optics + Photonics」にて発表する。



<量子エニグマ暗号トランシーバ (TU Cipher-0) >

【今回の成果】

データセンター間的高速光通信の安全性は、クラウド・システムのビジネス化を推進する上で最重要課題のひとつである。本学は、光通信システムの安全性を保証するための物理暗号の研究開発に取り組んできた。これまで、原理実証実験レベルにおいて最大 100 ギガビット毎秒の暗号通信を実現している。今回、デュアルユースでの実用を目指し、安全性を強化するランダム化機構を組み込んだギガビットイーサネット (GbE) 対応の量子エニグマ暗号トランシーバ (TU Cipher-0) を開発した。本トランシーバは、高さ 1U サイズ (約 44 mm) で 19 インチラックに設置可能。6月8～10日に幕張メッセで開催される「Interop Tokyo 2016^(注)」に出展 (展示ブース番号：4U09) し、「ShowNet^(注)」において相互接続検証を行う。また、技術詳細は、8月に米国サンディエゴで SPIE (国際光工学会) が開催する国際会議「SPIE Optics + Photonics」にて発表する。

【取材に関するお問い合わせ】

玉川学園教育企画部広報課

〒194-8610 東京都町田市玉川学園 6-1-1

電話 042-739-8710

E-mail : pr@tamagawa.ac.jp

【研究内容に関するお問い合わせ】

玉川大学 量子情報科学研究所

教授 二見 史生 (ふたみ ふみお)

研究室 電話:042-739-8644

E-mail: futami@lab.tamagawa.ac.jp

資料

【背景】

ネットの進展によって、データセンターを基盤とするクラウド・システムを用いたネットワークが急速に普及し始めている。クラウド・システムの安全保障においてはデータセンターの情報をバックアップするための通信回線(物理層)の保護は必須である。そのような機能開発として、2000年、米国 DARPA (国防高等研究計画局) は物理層の暗号、いわゆる物理暗号の開発を開始した。物理層を保護する物理暗号は光信号を正確にコピーさせないことによって安全性を担保するので、全ての通信情報を隠すことになる。その波及効果として、改ざんを阻止する事ができる。本学では、DARPA プロジェクト開発の物理暗号を改良し、大容量通信と安全性を両立する量子エニグマ暗号の理論・実験研究を推進してきた。これまでは原理実証実験を主に進めてきたが、今日、実利用している通信回線に導入できるトランシーバの開発が求められていた。

【開発したトランシーバ】

安全性を強化するランダム化機構を組み込んだ、ギガビットイーサネット(GbE)に対応する量子エニグマ暗号の送信機と受信機をワンボックスに収めた量子エニグマ暗号トランシーバ (TU Cipher-0) を作製した。本トランシーバは全二重通信可能で、ギガビットイーサネット(GbE)信号と物理暗号信号を相互に変換する。19 インチラック設置可能な幅で、高さは最小規格の 1U (約 44 mm) 【前頁写真参照】。本学キャンパス内の地下に敷設してある通信試験用の光ファイバ通信回線「TAMA Net #1」に導入し1ヶ月以上にわたりネット接続し、試験運用に成功している。ギガビットイーサネット通信回線の両端に本トランシーバを導入すると、暗号通信によって回線を保護できる。

■学会発表：SPIE(国際光工学会)が開催する国際会議「SPIE Optics + Photonics」

Quantum Communications and Quantum Imaging XIV, 2016.

- F. Futami, K. Kato, and O. Hirota, “A novel transceiver of the Y-00 quantum stream cipher with the randomization technique for optical communication with higher security performance,”
- K. Kato, “Quantum enigma cipher as a generalization of the quantum stream cipher,”

■注釈

Interop Tokyo : 世界で開催されているネットワークコンピューティングに特化したテクノロジーとビジネスのリーディングイベント。日本では1994年の初開催以来、2016年で23回目の開催を迎える。詳細は、公式サイト参照 (<http://www.interop.jp/top.html>)

ShowNet : Interop 会場内からインターネットに接続するためのネットワーク。単にネットワークの接続性を提供するだけでなく、2年後、3年後、さらに先に浸透するであろう技術を先駆けて挑戦し、「ネットワークの未来像」を示し、現段階での課題となる相互接続性の検証や、未来像に向けた課題の克服に向けたチャレンジが行われる。詳細は、公式サイト参照(<http://www.interop.jp/2016/shownet/>)

以上